



The Blue Book Project

Phase 2 to Phase 3 Transition Event



CNA

Agenda

- **Welcome and Introduction**
- **Phase 2 Summary**
- **CONOPS Overview**
- **Transitioning to Phase 3**
- **Closing Remarks**





The Blue Book Project

Opening Remarks

Shawn Talmadge, State Coordinator





The Blue Book Project

Opening Remarks

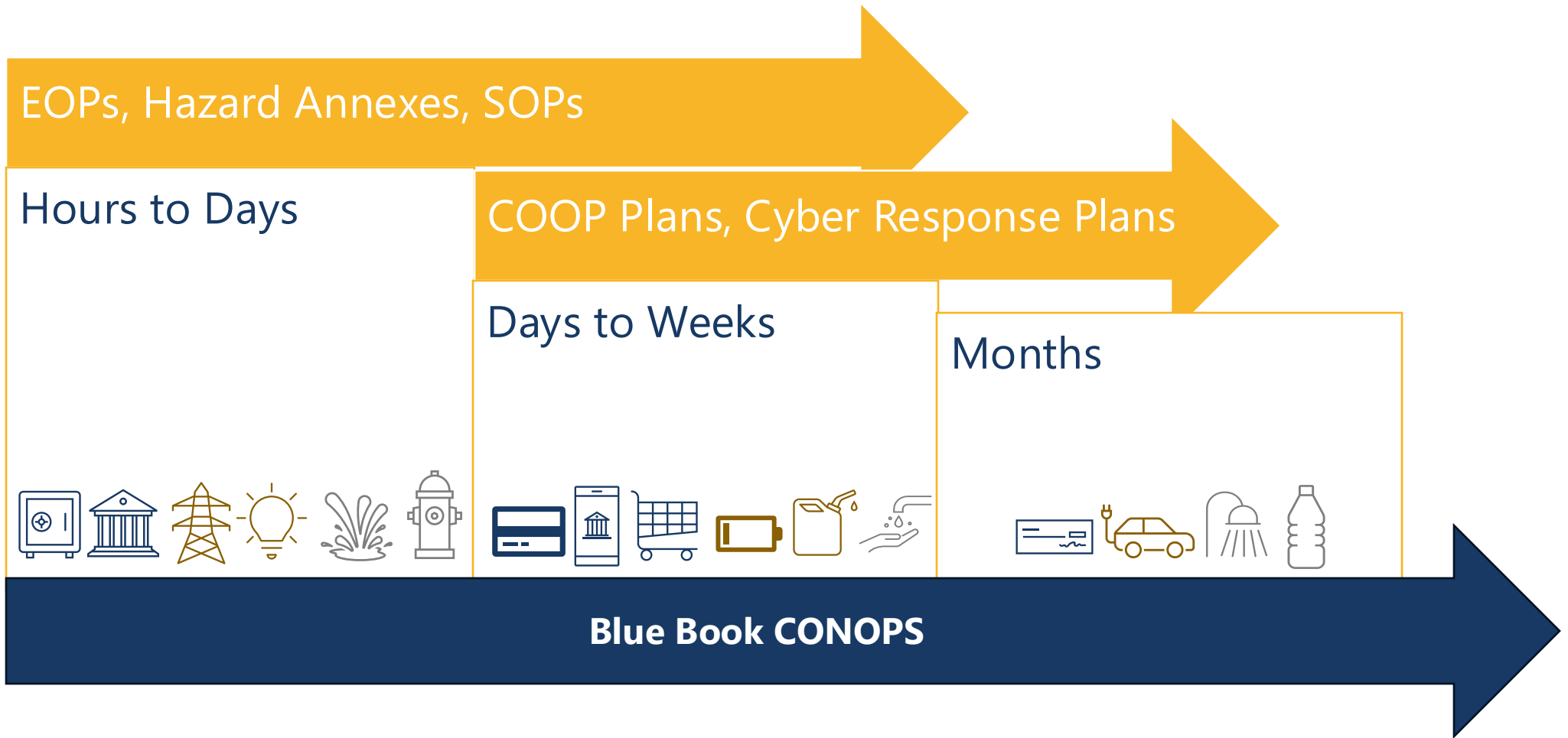
Tom Berry, Director of Planning



How the Blue Book Project is Different



CNA





COVEOP

Commonwealth of Virginia Emergency Operations Plan

Who: State Agencies
What: All Hazards
Why: Organize state response

Military

CI Owners and Operators

Private Sector

Local

Federal Partners

BLUE BOOK PROJECT

Who: VDEM and partners
What: Cyber attack on critical infrastructure
Why: Coordinate a complex, long-term response in a resource depleted environment

SUPPORT ANNEXES

Who: State Agencies
What: Specific Operations
Why: Organize and streamline state operations

HAZARD-SPECIFIC ANNEXES

Who: State Agencies
What: Individual Hazards
Why: Organize state response to those hazards

CYBER RESPONSE ANNEX

CONTINUITY OF GOVT

DISASTER FEEDING

VOLUNTEER AND DONATIONS MNGT

CONOPS

Who: VDEM, partners,
What: How to organize and respond to a cyber attack on CI.

SECTOR-SPECIFIC ANNEXES

SUPPORTING PLANS AND TOOLS

CONOPS TEMPLATE FOR LOCALS

Who: Local EM
What: How to organize and respond from a local perspective

WHITE PAPERS

Who: Anyone
What: Share findings, relevant research, and opportunities for stakeholders to better understand cyber threats and critical infrastructure.

*Examples of Support Annexes used in planning process



The Blue Book Project

Phase 2 Summary



CNA

BLUE BOOK PROJECT

STAKEHOLDER ENGAGEMENT IN NUMBERS

435
Total stakeholders engaged
since May 2024

Stakeholder Identification
239
partners identified

74 federal
93 state
19 local

44 private sector
9 other

Kickoff Event
80
attendees

Intelligence and Analysis 15
Consequence Management 53
Community Vulnerabilities 23

Critical Infrastructure and Private Sector 61
Military Requirements 27

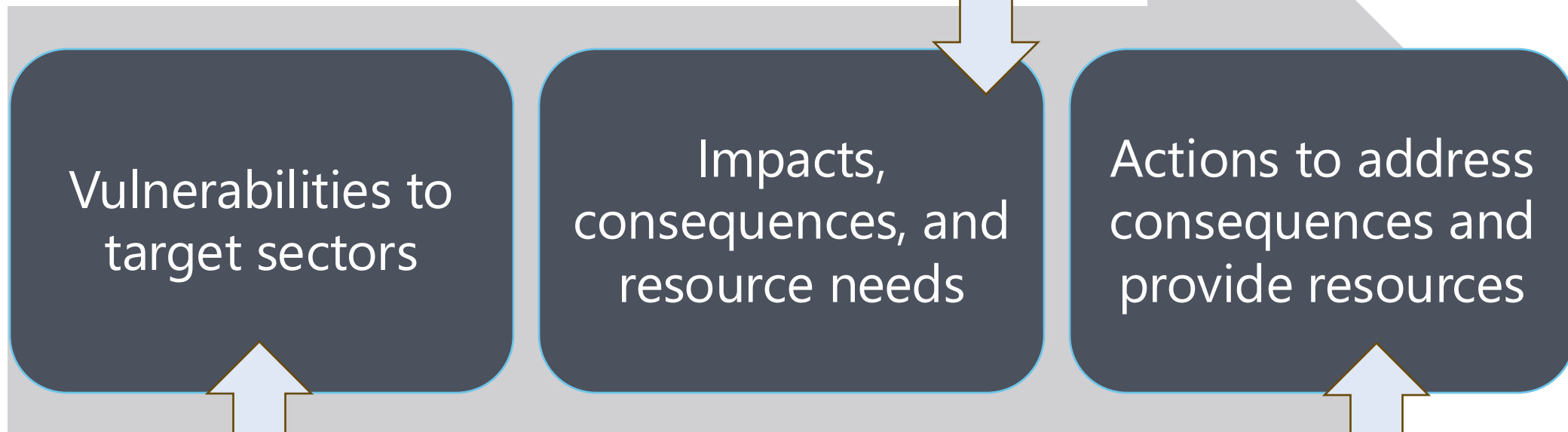
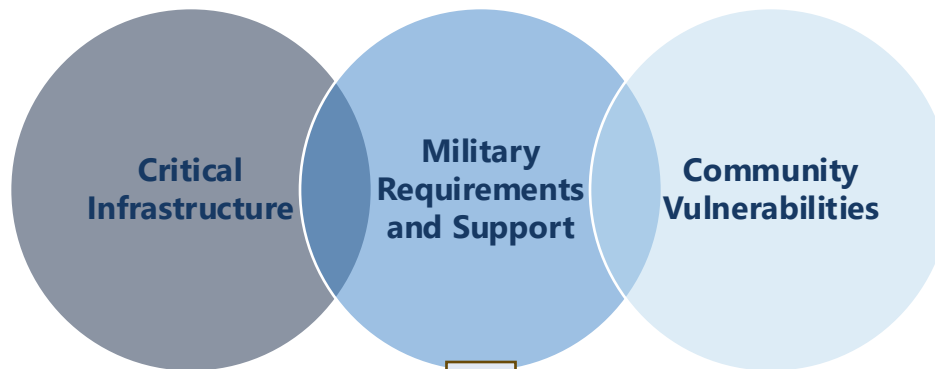
Working Group Meeting #1 Participation
179

Critical Infrastructure and Private Sector 50
Military Requirements 38

Working Group Meeting #2 Participation
176

Intelligence and Analysis 20
Consequence Management 47
Community Vulnerabilities 21

Phase 2 Working groups



Terms



CNA

Target Sectors: The critical infrastructure sectors that the Blue Book Project is focusing planning efforts around.

Impacts: The significant or major effects of a targeted attack.

- All internet providers are down in a region.
- Running water is not potable in eight counties.

Consequences: The situations/challenges resulting from an impact.

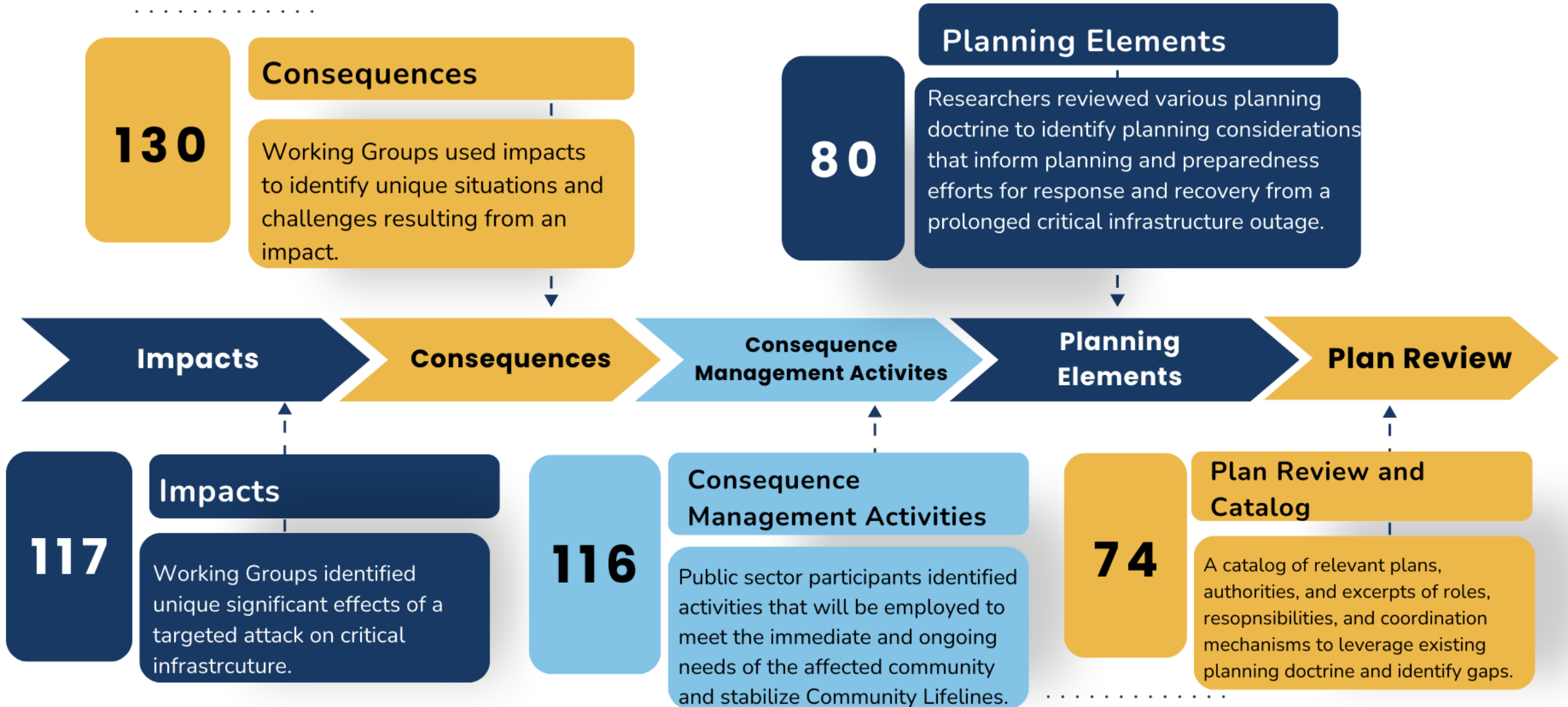
- Hospitals cannot use electronic medical records, order pharmaceuticals, send/receive images, etc.
- Schools need an alternate water supply for students.

Consequence Management Activities: Public sector activities employed to meet the immediate and ongoing needs of the affected community and stabilize the affected Community Lifelines.

- Deploy Starlink for essential operations and support hospitals in developing internet operations prioritization.
- Deploy tankers and bottled water to school.



BLUE BOOK PROJECT RESEARCH AND DATA COLLECTION





The Blue Book Project

Working Group Feedback: Consequences and Consequence Management Activities



Consequences – Examples by Lifeline



- Strain on emergency services due to increased call volume.
- Security concerns due to increased civil unrest and public distrust.



- Increased fatality management requirements due to energy loss during extreme heat or cold.
- Increased stress on the healthcare system due to prolonged outages of critical services.
- Disruption to public's ability to access critical service due to impacted medical facility operations.
- People with specialized health and medical dependencies are at imminent risk due to service disruptions to accessibility of essential and life-sustaining medical equipment.

Consequences are the situation or challenges resulting from the impacts.



Consequences – Examples by Lifeline



- Shortages in supply chains lead to increased competition for food in the community.
- Responding organizations experience severe shortages of the resources and equipment they require to activate PODs.



- Confusion and distrust amongst the public due to weaponized MDM campaigns.
- More difficult operational environment for communicating with vulnerable populations.
- Loss of standard communications methods with the public due to prolonged outages.
- Loss of standard emergency response communications methods leads to longer emergency response times.



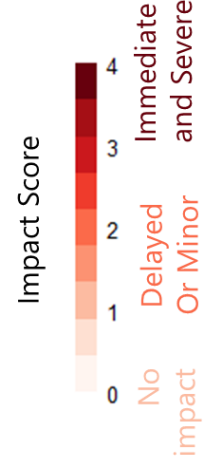
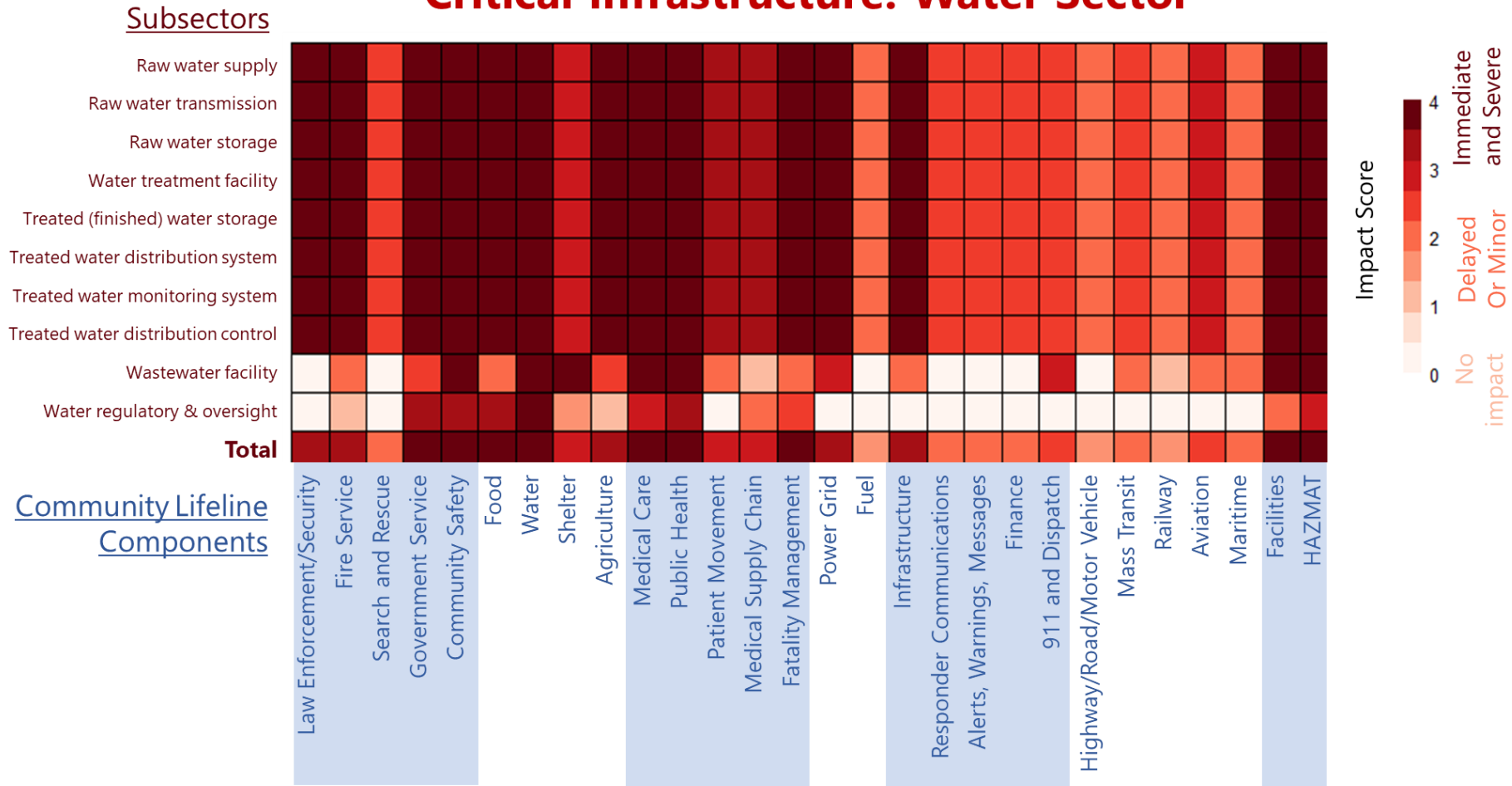
- Schools and businesses without power have difficulty staying open.
- Disruption of fuel supply chains limits essential firefighting, EMS, and military operations.
- Generators become a scarce resource and must be prioritized.



Consequences to Lifeline Components



Critical Infrastructure: Water Sector



This heatmap describes how outages in critical infrastructure subsectors may impact community lifeline components.



Consequence Management Activities



CNA

- Activate plans
 - COOP
 - Sheltering
 - PODs
- Activate operational coordination structure
- Establish resource prioritization process (e.g., for fuel, generators, access to roadways)
- Deploy generators and other resources
- Operate POD sites
- Consolidate 911 centers
- Upstaff call centers
- Coordinate with fuel suppliers
- Leverage amateur radio communications
- Activate alternative water options (desalinization, bottled water, etc.)
- Activate volunteer and donations management plans
 - Engage CERT Teams
 - Identify additional volunteer base sources
- Launch public water safety campaigns
- Secure and utilize additional security contracts
- Coordinate with healthcare coalitions
- Engage communications strategies against MDM

Activities that will need to be conducted to manage the consequences of a major cyberattack.



The
Blue Book Project

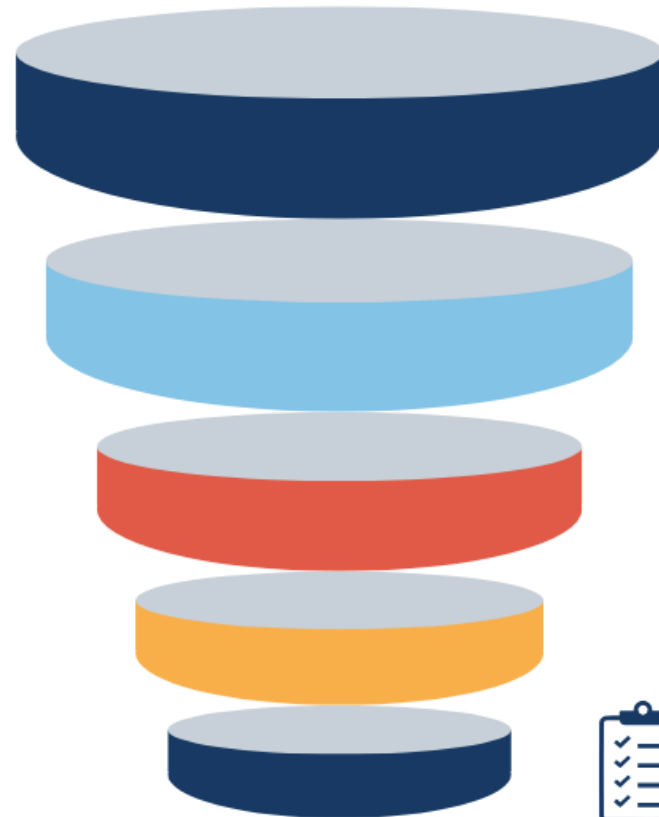


Putting it all together



CNA

Blue Book Phase 2 Findings



Understand Vulnerabilities

Complex coordinated cyberattack on one or more CI sectors



Identify Impacts

Severely damaged and destroyed critical infrastructure



Determine Consequences

Business and school closures, strained emergency services, supply chain disruptions




Identify Consequence Management Activities

Bottled water distribution, food distribution, military coordination




Establish Mission Areas


Mission Areas



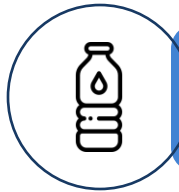
Continuity of Government



Alternative Sources and Supply Chains for Key Resources




Public Information



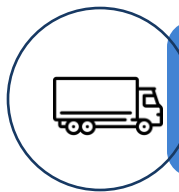
Continuity of the Private Sector




Resource Distribution / PODs



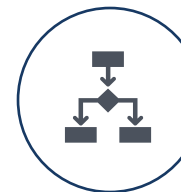
Policy



Military Coordination



Volunteer Identification and Management



Operational Coordination

Mission areas are a refined list of consequence management activities that will be key to managing consequences and complex operations due to degraded conditions.





The Blue Book Project

Transition to Phase 3



CNA

Phase 3 and 4 Execution



RESEARCH AND ENGAGEMENT

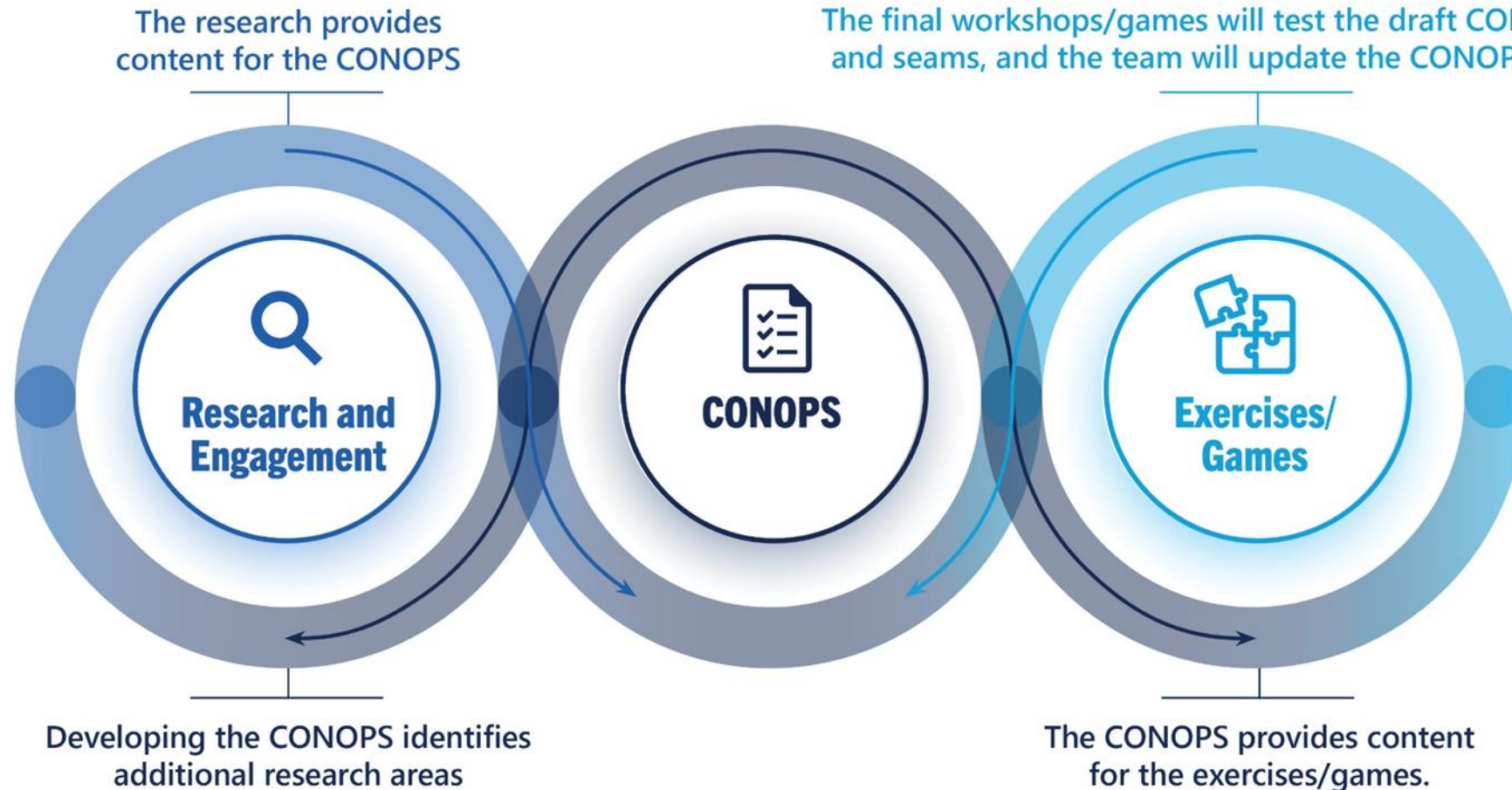
Exploring the history of Civil Defense; planning factors for large mission areas; relevant legislations, authorities, and regulations; impacts and cascading effects on critical infrastructure, etc. Engage SME (including from the private sector) to best integrate research into planning process.

CONOPS

Documenting the framework to support the response and recovery, the missions that need to be carried out, the structure and processes for decision-making and prioritization.

EXERCISES/GAMES

Immerse project partners in workshops and games to explore specific missions, concepts, and challenges for managing the consequences that could arise during large-scale and prolonged outages of critical infrastructure services.





The Blue Book Project

Concept of Operations



Concept of Operations



CNA

Purpose

To establish a coordinated operational process to support local, state, federal, military, and private sector priorities, support Virginia residents and visitors, and ensure continuity of government during a coordinated cyberattack on critical infrastructure systems.

Scope

- Timeframe: Hour 0 through Six Months
- Critical Infrastructure Sectors: Water, Power, Transportation, Telecommunications, Financial Systems
- User: State Agencies

Assumptions

- Full VEST activation
- Long-term disruptions to multiple critical infrastructure sectors
- Resource scarcity will pose unique challenges to NIMS assumptions
- Military installations will require state support in order to continue to fulfill missions
- National Guard resources will be required to support Title X mission



CONOPS Outline



CNA

- **Introduction**
 - Purpose
 - Scope
- **Definitions**
- **Situation Overview**
- **Assumptions**
- **Goals and Objectives**
- **Concept of Operations**
- **Organization and Assignment of Responsibilities**
- **Direction, Control, Coordination**
- **Plan Development and Maintenance**
- **Authorities and References**
- **5 Sector-Specific Annexes**



Concept of Operations

Concept of Operations Section

- **General**
- **Pre-Incident Actions**
- **Initial Response**
- **Sustained Response**
 - (9) Mission Areas
- **Transition to Recovery**



Goals 1 and 2



CNA

- **Goal 1: Safeguard Public Safety and Maintain Public Trust**
 - **Objective 1.1:** Support the ongoing delivery of and access to emergency services that prioritize life-safety and life sustainment.
 - **Objective 1.2:** Develop and implement prevention strategies to mitigate civil unrest and address public disturbances, maintaining public order and fostering a safe and secure environment within the affected communities.
 - **Objective 1.3:** Establish and maintain processes that protect and prioritize response to vulnerable populations.
 - **Objective 1.4:** Maintain clear and consistent communication with the public, providing timely updates and guidance to reduce panic and build trust.
- **Goal 2: Ensure Continuity of Essential Services**
 - **Objective 2.1:** Coordinate with service providers to support efforts to limit the duration and severity of disruptions to essential services during an infrastructure outage.
 - **Objective 2.2:** Coordinate with key service providers to implement response measures that address government, public, and military needs to restore essential services.
 - **Objective 2.3:** Coordinate with public and private sector to provide resources needed to continue operating in a degraded environment.



Goals 3 and 4



CNA

- **Goal 3: Provide Support that Enables Military Operation Sustainment**
 - **Objective 3.1:** Identify opportunities for state support that enable military installations to sustain missions.
 - **Objective 3.2:** Coordinate assets and resources to support the Department of Defense and other military partners in ensuring operational readiness.
- **Goal 4: Facilitate Rapid Recovery**
 - **Objective 4.1:** Coordinate with public and private sector partners to understand recovery needs and develop a recovery plan informed by feedback that expedites the start of the recovery process.
 - **Objective 4.2:** Support recovery planning that includes both public and private partners early in response to restore critical infrastructure efficiently and reduce downtime.
 - **Objective 4.3:** Minimize the disruption to essential services and daily life for citizens and businesses.

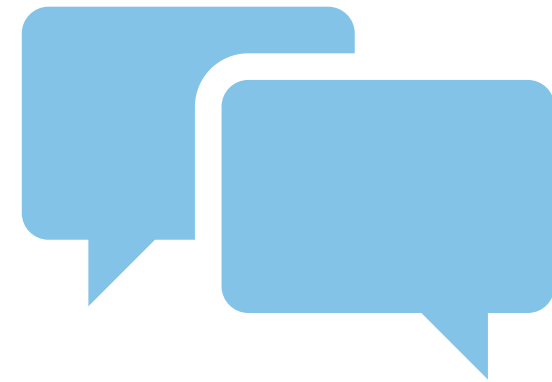


CONOPS Goals and Objectives Activity



CNA

Go to [menti.com](https://www.menti.com) and use code 8506 0210





The Blue Book Project

Phase 3: Mission Areas



Purpose of the Mission Areas



CNA

To outline potential (or promising) approaches to address the anticipated complex consequence management efforts in a degraded and resource depleted environment.

- **Why?**

- This scenario is unlike any other incident
- Current plans and operations will serve as a starting point, but response will need to be scaled up (Initial Response)
- Geographic scope, incident complexity, and outage duration will require new approaches to operations over time (Prolonged Response)



Mission Area Content



Continuity of Government

- Government functions in a constrained environment
- Workforce management



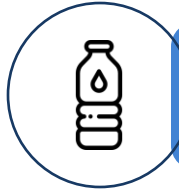
Alternative Sources and Supply Chains for Key Resources

- Electricity, water, communications, food, and fuel



Public Information

- Countering MDM
- Controversial topics, e.g., rationing
- Coordinated messaging



Continuity of the Private Sector

- Private sector engagement
- Workforce management
- Resource needs



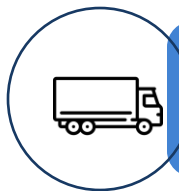
Resource Distribution / PODs

- Distribution of resources, e.g., mass feeding
- Equity considerations



Policy

- Policies, legislation, regulation, funding mechanisms, authorities, and waivers



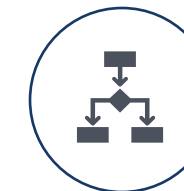
Military Coordination

- Communication and coordination
- Resource support



Volunteer Identification and Management

- Identifying and training volunteers
- Volunteer management



Operational Coordination

- Response / VEST structure
- Resource prioritization
- Multi-agency coordination



Mission Area Workshops

What: Focused scenario-based activities

When: December - March

Why: Assemble a group with experience or expertise around a mission to discuss anticipated challenges and identify potential solutions, workarounds, or adjustments to ensure the mission can continue in a degraded environment.

How:

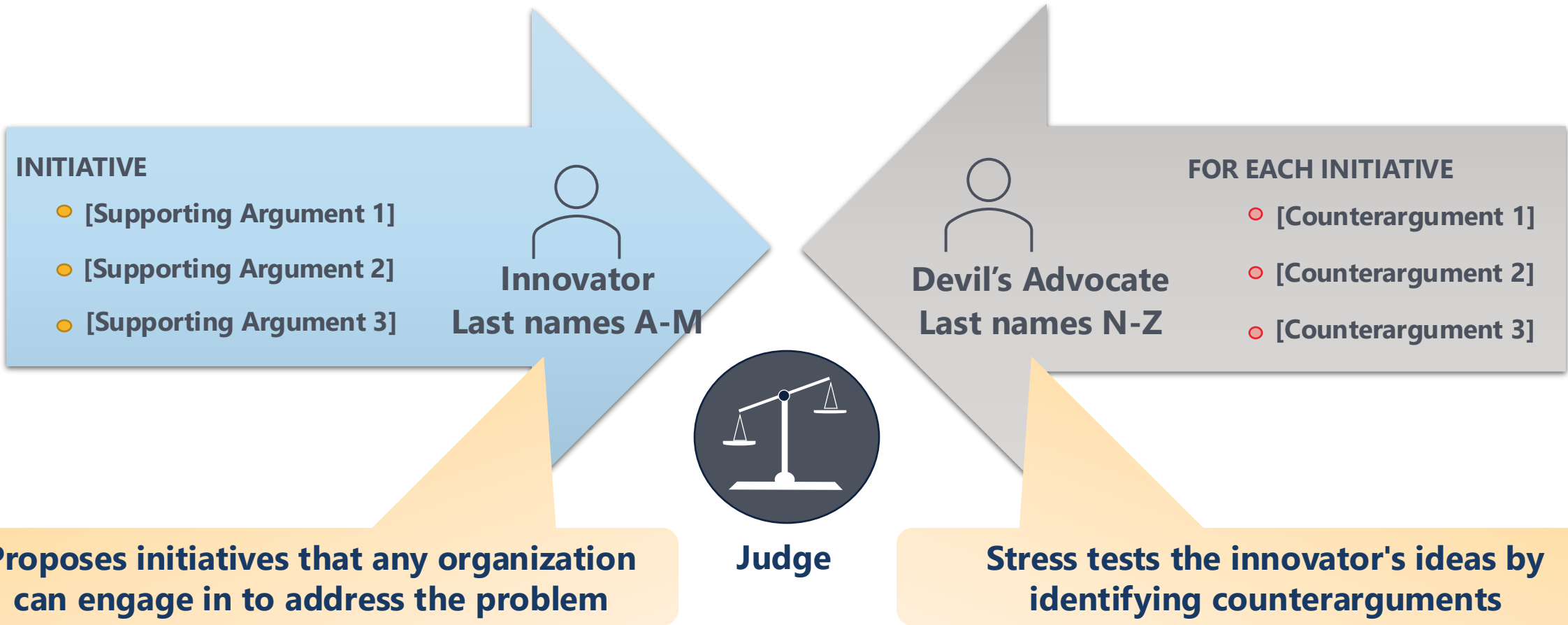
- Small-group discussions
- Serious games
- Structured debates (aka Matrix games)



Matrix Games Demo: Youth Online Bullying



CNA





The Blue Book Project

Phase 3 Engagement



Mission Areas Sign Up

Continuity of Government

- Government functions in a constrained environment
- Workforce management

Alternative Sources and Supply Chains for Key Resources

- Electricity, water, food, communications, and fuel
- Includes reducing demand

Public Information

- Countering MDM
- Controversial topics, e.g., rationing
- Coordinated messaging

Continuity of the Private Sector

- Private sector engagement
- Workforce management
- Resource needs

Resource Distribution / PODs

- Distribution of resources, e.g., mass feeding
- Equity considerations

Policy

- Policies, legislation, regulation, funding mechanisms, authorities, and waivers

Military Coordination

- Communication and coordination
- Resource support

Volunteer Identification and Management

- Identifying and training volunteers
- Volunteer management

Operational Coordination

- Response / VEST structure
- Resource prioritization
- Multi-agency coordination

Blue Book Mission Areas Submission of Interest



<https://forms.office.com/g/Buu2g0Gpts>

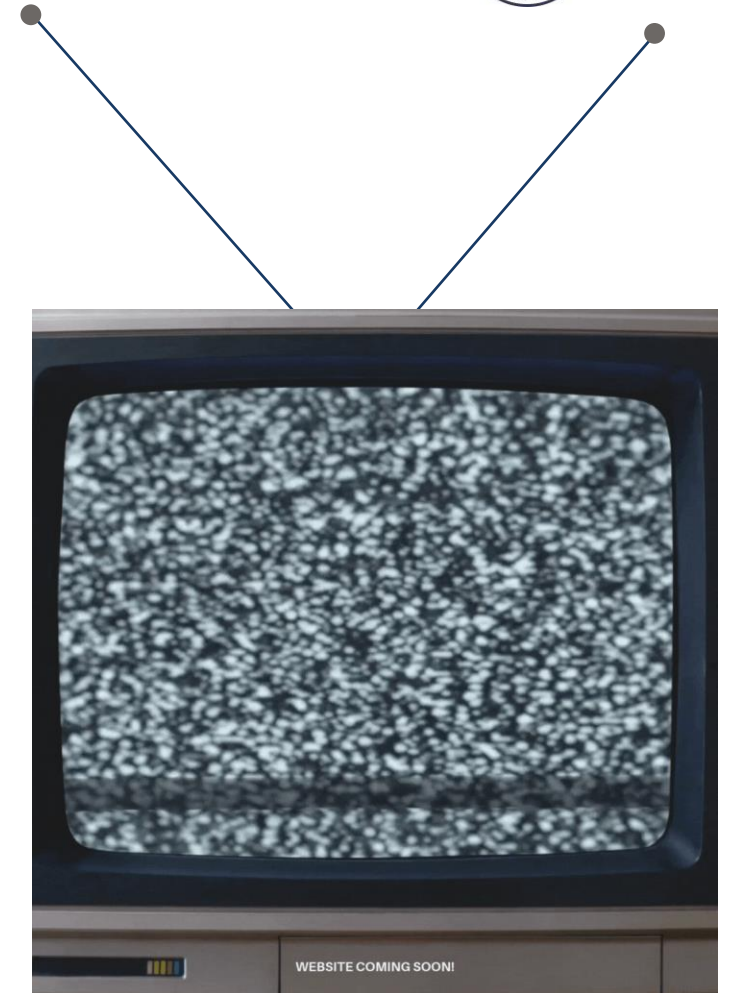


Blue Book TV



CNA

- **Virtual Event**
- **First Tuesday of every month from 12-1:30pm**
- **Confirmed and potential future topics**
 - Mis-, Dis-, and Mal-information (**December 3rd at noon**)
 - During the Blue Book scenario
 - Tips and tricks for addressing it
 - National Emergency Civil Defense Panel Discussion: FEMA, VDEM, NAS Oceanna
 - Target Sector Threat Briefs
 - Houston RCPG planners
 - Hurricane Helene Response Best Practices and Lessons Learned (for long-term lifeline outages)



The
Blue Book Project



White Papers



CNA

Completed:

- VDEM Blue Book Overview
- Lessons Learned from Phase 1
- Overview and Application of the Defense Production Act
- MDM Information 101 for Emergency Managers
- How to Increase Resilience Against Disinformation
- Civil Defense: From the Cold War to Contemporary Threats



In-Progress

- Law Enforcement Support to Military Installations
- Innovations in Consequence Management
- Target Sector Threat Summaries
- Lessons Learned from Phase 2
- Critical Infrastructure Dependencies and Interdependencies

How to Access White Papers: <https://www.vaemergency.gov/blue-book>



Closing Remarks

